

AO 91 (Rev. 08/09) Criminal Complaint

## UNITED STATES DISTRICT COURT

FILED 05 JUN 13 10:26 USDC-ORE

for the

District of Oregon

United States of America )  
 v. )  
 Jenelle Robyn Pinkston )  
 )  
 )  
 )  
 )

Case No. 6:13-mj-85-TC

*Defendant(s)*

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 16, 2013 and May 23, 2013 in the county of Linn in the  
 District of Oregon, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
Title 18 U.S.C Section 844(e)	Threatening the use of an explosive device to damage or destroy a building in interstate commerce

This criminal complaint is based on these facts:

See attached affidavit which is attached hereto and incorporated herein by this reference.

Continued on the attached sheet.



Complainant's signature

Timothy W. Suttles, Special Agent, FBI*Printed name and title*

Sworn to before me and signed in my presence.

Date: 06/05/2013



Judge's signature

City and state: Eugene, Oregon

Thomas M. Coffin, U.S. Magistrate Judge*Printed name and title*

**ATTACHMENT B**

**I. Items to be Searched For, Seized, and Examined**

The items to be searched for, seized and examined are those items on the Device, referenced in Attachment A, that contains evidence and instrumentalities of the following crime: threatening the use of an explosive device to damage or destroy a building in interstate commerce in violation of Title 18, U.S.C. § 844(e).

1. The items referenced above to be seized and examined are as follows:

- A. The Device, as it appears to be capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence or instrumentalities of such crimes;
- B. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
- C. All records, documents, programs, applications, or materials created, modified, or stored in any form, that show the actual user(s) of the Device during any time period in which the Device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used; MAC IDs and/or Internet Protocol addresses used by the Device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

D. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

E. Records and things evidencing Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

## **II. Search Procedure**

1. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

A. Law enforcement personnel will examine the Device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in this attachment. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

B. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a Ahash value@ library to exclude normal operating system files that do not need to be searched. In

addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

C. Law enforcement personnel will perform an initial search of the original Device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that the Device or image contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the Device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether the Device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the Device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

D. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law

enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

E. If the Device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return the Device to its owner within a reasonable period of time following the search of the Device and will seal any image of the Device, absent further authorization from the Court.

STATE OF OREGON )  
                      )  
                      ) AFFIDAVIT OF TIMOTHY W. SUTTLES  
County of Lane     )

**Affidavit in Support of an Application**  
**for a Complaint, an Arrest Warrant and a Warrant to Search and Seize Evidence Including**  
**Digital Data**

I, Timothy W. Suttles, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1. I am a Special Agent of the Federal Bureau of Investigation, and have been so employed for over 12 years. As a Federal Agent, I am authorized to investigate violations of laws of the United States. My responsibilities include the investigation of federal criminal violations. In the course of my employment with the FBI, I have participated in the execution of numerous search warrants resulting in the seizure of computers and electronic media, as well as other items evidencing violations of federal laws.

2. This affidavit is submitted in support of an application for a complaint, an arrest warrant and a search warrant for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 844(e), threatening the use of an explosive device to damage or destroy a building in interstate commerce.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of one Black LGL55C cell phone S/N: 110KPPB0059336, hereinafter "Device," which is currently stored, in law enforcement possession, in the Evidence Control Room of the Albany Police Department, 1117 Jackson Street SE, Albany, Oregon, as described in Attachment A which is attached hereto and

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 1

USAO Version Rev. Mar. 2013

incorporated herein by this reference, and the extraction from the Device of certain things described in Attachment B which is also attached hereto and incorporated herein by this reference. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence of violations of Title 18, U.S.C. Section 844(e).

4. The facts set forth in this affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause, it does not set forth each and every fact that I or others have learned during the course of this investigation.

**Applicable Law**

5. Title 18, U.S.C. Section 844(e) provides that one has violated this section if: Whoever, through the use of the mail, telephone, telegraph, or other instrument of interstate or foreign commerce, or in or affecting interstate or foreign commerce, willfully makes any threat, or maliciously conveys false information knowing the same to be false, concerning an attempt or alleged attempt being made, or to be made, to kill, injure, or intimidate any individual or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of fire or an explosive.

**Statement of Probable Cause**

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 2

USAO Version Rev. Mar. 2013

6. On April 16, 2013, at approximately 1:20 PM, Waverly Elementary School, 425 SE Columbus Street, Albany, Oregon, contacted 911 and reported a bomb threat. The caller to 911 stated a person with a male raspy voice said the bomb would go off in 10 minutes. As a result of the bomb threat the fire alarm was activated and approximately 270 students and staff evacuated the building. Responding officers attempted to dial \*69 on the school phone system but were unsuccessful because parents of students at the school had flooded all of the school telephone lines in response to the evacuation. Responding officers performed a safety sweep and determined the building and grounds were safe.

7. Linn County Sheriff's Detective Micah Smith told me that he contacted Integra, the telephone service provider for Waverly Elementary School, as well as several other schools in the Greater Albany School District. Detective Smith learned that the number which called in the bomb threat was (541) 730-9207. Integra was able to search incoming calls to the school and identify the number based on the time the call was received. Detective Smith checked Linn County Sheriff's Office and Albany Police Department records but was unable to identify any contact with telephone number (541) 730-9207. Detective Smith identified that the telephone number was service by Sprint. Detective Smith sent a subpoena to Sprint for subscriber information for (541) 730-9207.

8. On May 23, 2013, at approximately 12:21 PM, Albany Police Dispatch 911 received a call from Waverly Elementary School reporting a telephonic bomb threat. The caller to 911 stated a person with a male raspy voice said the bomb would go off in 15 minutes. As a result of the bomb threat the fire alarm was activated and approximately 270 students and staff evacuated

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 3

USAO Version Rev. Mar. 2013

the building. Responding officers performed a safety sweep and determined the building and grounds were safe.

9. Detective Smith responded to the scene and contacted Integra. Detective Smith was informed that the number which called in the bomb threat was (541) 730-9207. Detective Smith contacted Sprint in an attempt to identify the subscriber to telephone number (541) 730-9207.

10. On May 23, 2013, at approximately 1:24 PM, Albany Police Dispatch 911 received a call from Periwinkle Elementary School, 2196 21<sup>st</sup> Avenue, Albany, Oregon, reporting a telephonic bomb threat. Detective Smith contacted Integra and learned that the number which called in the bomb threat was (541) 730-9207.

11. Detective Smith contacted Sprint's Emergency Response team via their toll-free number requested Call Detail Records for telephone number (541) 730-9207. Detective Smith established with Sprint that the information was based on an exigency necessity. Detective Smith was able to identify a common number pattern used by phone number (541) 730-9207. One common number that was contacted by both voice and text message was (541) 979-5775.

12. Detective Smith search Linn County Sheriff's Office records and located that phone number (541) 979-5775 was associated with Courtney Pinkston with an address on SE 4<sup>th</sup> Avenue, Albany, Oregon. This location is directly across the street from Waverly Elementary School. Detective Smith contacted TracFone on their Law Enforcement Line as TracFone is the information custodian of record for telephone number (541) 730-9207. After explaining the exigency of the situation, Detective Smith was advised that telephone number (541) 730-9207, was subscribed to by Jenelle Pinkston, with a date of birth of XX/XX/1967. TracFone provided an

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 4

USAO Version Rev. Mar. 2013

address of 415 Williams Avenue, Madison, Tennessee 37115. Detective Smith located and talked to Courtney Pinkston who told him that Jenelle Pinkston was her mother and was currently living at 2305 SE 4<sup>th</sup> Avenue, Albany, Oregon.

13. Detective Smith and Albany Police Officer Curtis Bell located and interviewed Jenelle Pinkston at 2305 SE 4<sup>th</sup> Avenue, Albany, Oregon. Detective Smith told me that during the interview, Jenelle Pinkston denied making the threat calls to the schools. Detective Smith asked Jenelle Pinkston if he could look though her phone, described as one Black LGL55C cell phone S/N: 110KPPB0059336. Jenelle Pinkston consented to the search. Detective Smith found no calls in the call history. Detective Smith found that the web browser history showed she had searched for contact information for Periwinkle Elementary School. Jenelle Pinkston told Detective Smith that she had to call the school to verify that it was alright for her to bring cupcakes to her grandson's classroom for his birthday.

14. Jenelle Pinkston was told that Call Detail Records for her phone showed that she called Waverly Elementary School twice and Periwinkle Elementary School once at the same time that a bomb threat was reported by the schools. During the ongoing interview Jenelle Pinkston confessed to making the two bomb threat calls, one to Waverly Elementary School and one to Periwinkle Elementary School. She said during the interview that she did not recall making the bomb threat call to Waverly Elementary School on April 16, 2013.

15. During the interview Officer Bell asked Jenelle Pinkston if she used an electronic device to disguise her voice and she said she did not have any such device. Officer Bell asked if she could talk in a really high voice and she demonstrated that she could. Officer Bell asked if she

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 5

USAO Version Rev. Mar. 2013

could talk in a really low voice and she demonstrated that she could also do that.

16. Janelle Pinkston was arrested and transported to the Linn County Jail. She has been charged with three counts of Coercion, three counts of Disorderly Conduct, and two counts of Tampering with Evidence. She is currently still in custody in Linn County.

17. I reviewed Jenelle Pinkston's criminal history and discovered the following: on March 11, 1988, in Lane County Circuit Court, she was convicted of two counts of Arson in the 2nd Degree. She was sentenced to 30 days in jail and five years probation. On August 5, 1998, Pinkston was arrested at Oregon State University for two counts Criminal Conspiracy, Burglary, Computer Crimes, and Forgery. Those charges were dismissed on November 21, 2003. On May 14, 1999, Pinkston was sentenced to four years in prison for two counts of Forgery in Kingsport, Tennessee. On December 18, 2002, Pinkston was sentenced to six years in prison for Arson in Smyrna, Tennessee. During the initial arrest, she was also charged with making Bomb Threats. Those charges were dismissed.

**Item to be Searched**

18. I make this affidavit in support of the issuance of a search warrant for one Black LGL55C cell phone S/N: 110KPPB0059336, currently in the Evidence Control Room at the Albany Police Department.

**Items to be Seized**

19. Based on my training and experience, and my knowledge of this investigation, I have probable cause to believe, and do believe, that the following evidence and instrumentalities of the crime under investigation are currently located within one Black LGL55C cell phone S/N:

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 6

USAO Version Rev. Mar. 2013

110KPPB0059336. These items include call logs/history, text messages, web searches and history, and any additional digital data associated with the commission of the crime being investigated.

20. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

**Search and Seizure of Digital Data**

21. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

22. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

**Removal of Data Storage Devices**

23. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during the search of the premises it is not always possible to create a forensic image of

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 7

USAO Version Rev. Mar. 2013

or search digital devices or media for data for a number of reasons, including the following:

- A. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.
- B. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.
- C. The volume of data stored on many digital devices is typically so large that it will be highly impractical to search for data during the execution of the physical search of the premises. Storage devices capable of storing 500 gigabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

**Laboratory Setting May Be Essential For Complete And Accurate Analysis Of Data**

24. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 8

USAO Version Rev. Mar. 2013

complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

25. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 9

USAO Version Rev. Mar. 2013

was sitting at the keyboard.

26. *Latent Data:* Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after having been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

27. *Contextual Data:*

A. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 10

USAO Version Rev. Mar. 2013

user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

B. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

C. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 11

USAO Version Rev. Mar. 2013

digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

#### **Search Procedure**

28. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

A. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 12

USAO Version Rev. Mar. 2013

be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

B. *On-site imaging, if practicable.* If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.

C. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

D. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

E. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 13

USAO Version Rev. Mar. 2013

seized under the warrant.

F. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

G. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 14

USAO Version Rev. Mar. 2013

enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

H. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

**Data to be Seized**

29. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

A. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

B. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 15

USAO Version Rev. Mar. 2013

above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

C. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

D. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

E. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

F. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

G. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

H. All records, documents, programs, applications, or materials created, modified, existing or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to commit the crimes referenced above, including

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 16

USAO Version Rev. Mar. 2013

the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

30. The government has made the following prior efforts in other judicial fora to obtain evidence sought in the warrant: grand jury subpoenas and exigent information request.

**Retention of Image**

31. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

**Inventory and Return**

32. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

**Conclusion**

33. Based on the foregoing, I have probable cause to believe, and I do believe, that

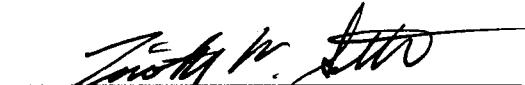
AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 17

USAO Version Rev. Mar. 2013

Jenelle Pinkston willfully threatened the use of an explosive device to damage or destroy a building in interstate commerce in violation of Title 18, U.S.C. Section 844(e), and that evidence and instrumentalities of that offense, as more fully described in Attachment B hereto, are presently located in one Black LGL55C cell phone S/N: 110KPPB0059336. I therefore request that the court issue a warrant authorizing the arrest of Jenelle Pinkston and a search of one Black LGL55C cell phone S/N: 110KPPB0059336 for the items listed in Attachment B, and the seizure and examination of any such items found.

34. This affidavit, the accompanying application, and the requested arrest warrant and search warrant were all reviewed by Assistant United States Attorney (AUSA) William Fitzgerald prior to being submitted to the court. AUSA Fitzgerald informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

  
\_\_\_\_\_  
Timothy W. Suttles  
Special Agent, FBI

Subscribed and sworn to before me this 5 day of June, 2013.

  
\_\_\_\_\_  
Thomas M. Coffin  
United States Magistrate Judge

AFFIDAVIT OF TIMOTHY W. SUTTLES

Page 18

USAO Version Rev. Mar. 2013

**ATTACHMENT A**

**DIGITAL DEVICE(S) TO BE SEARCHED**

The digital device to be searched is one Black LGL55C cell phone S/N: 110KPPB0059336 and is currently located on the premises of the Albany Police Department, 1117 Jackson Street SE, Albany, Oregon.

**ATTACHMENT B**

**I. Items to be Searched For, Seized, and Examined**

The items to be searched for, seized and examined are those items on the Device, referenced in Attachment A, that contains evidence and instrumentalities of the following crime: threatening the use of an explosive device to damage or destroy a building in interstate commerce in violation of Title 18, U.S.C. § 844(e).

1. The items referenced above to be seized and examined are as follows:
  - A. The Device, as it appears to be capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence or instrumentalities of such crimes;
  - B. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
  - C. All records, documents, programs, applications, or materials created, modified, or stored in any form, that show the actual user(s) of the Device during any time period in which the Device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used; MAC IDs and/or Internet Protocol addresses used by the Device; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

D. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

E. Records and things evidencing Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

## **II. Search Procedure**

1. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

A. Law enforcement personnel will examine the Device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in this attachment. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

B. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a Ahash value@ library to exclude normal operating system files that do not need to be searched. In

addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

C. Law enforcement personnel will perform an initial search of the original Device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that the Device or image contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the Device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether the Device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the Device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

D. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law

enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

E. If the Device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return the Device to its owner within a reasonable period of time following the search of the Device and will seal any image of the Device, absent further authorization from the Court.